ISO 26262

From Wikipedia, the free encyclopedia

Parts of this article (those related to part 2 to part 9 of the standard) need to be **updated**. Please help update this article to reflect recent events or newly available information.
Last update: 2011 *(November 2018)*

ISO 26262, titled "Road vehicles - Functional safety", is an international standard for functional safety of electrical and/or electronic systems that are installed in serial production road vehicles (excluding mopeds), defined by the International Organization for Standardization (ISO) in 2011, and revised in 2018.

Overview of the Standard [edit]

Functional safety features form an integral part of each automotive product development phase, ranging from the specification, to design, implementation, integration, verification, validation, and production release. The standard ISO 26262 is an adaptation of the Functional Safety standard IEC 61508 for Automotive Electric/Electronic Systems. ISO 26262 defines functional safety for automotive equipment applicable throughout the lifecycle of all automotive electronic and electrical safety-related systems.

The first edition (ISO 26262:2011), published on 11 November 2011, was limited to electrical and/or electronic systems installed in "series production passenger cars" with a maximum gross weight of 3,500 kilograms (7,700 lb). The second edition (ISO 26262:2018), published in December 2018, extended the scope from passenger cars to all road vehicles except mopeds.[1]

The standard aims to address possible hazards caused by the malfunctioning behaviour of electronic and electrical systems in vehicles. Although entitled "Road vehicles - Functional safety" the standard relates to the functional safety of Electrical and Electronic systems as well as that of systems as a whole or of their mechanical subsystems.

Like its parent standard, IEC 61508, ISO 26262 is a risk-based safety standard, where the risk of hazardous operational situations is qualitatively assessed and safety measures are defined to avoid or control systematic failures and to detect or control random hardware failures, or mitigate their effects.

Goals of ISO 26262:

- Provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases.
- Covers functional safety aspects of the entire development process (including such activities as requirements specification, design, implementation, integration, verification, validation, and configuration).
- Provides an automotive-specific risk-based approach for determining risk classes (Automotive Safety Integrity Levels, ASILs).
- Uses ASILs for specifying the items' necessary safety requirements for achieving an acceptable residual risk.
- Provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety is being achieved.[2]

Parts of ISO 26262 [edit]

ISO 26262:2018 consists of twelve parts, ten normative parts (parts 1 to 9 and 12) and two guidelines (parts 10 and 11): [*citation needed*]

1. Vocabulary
2. Management of functional safety
3. Concept phase
4. Product development at the system level
5. Product development at the hardware level
6. Product development at the software level
7. Production, operation, service and decommissioning
8. Supporting processes
9. Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analysis
10. Guidelines on ISO 26262
11. Guidelines on application of ISO 26262 to semiconductors
12. Adaptation of ISO 26262 for motorcycles

In comparison, ISO 26262:2011 consisted of just 10 parts, with slightly different naming:

- Part 7 was named just *Production and operation*
- Part 10 was named *Guideline …* instead of *Guidelines …*
- Parts 11 and 12 did not exist.

Part 1: Vocabulary [edit]

ISO 26262 specifies a vocabulary (a Project Glossary) of terms, definitions, and abbreviations for application in all parts of the standard.[1] Of particular importance is the careful definition of *fault*, *error*, and *failure* as these terms are key to the standard's definitions of functional safety processes,[3] particularly in the consideration that "A *fault* can manifest itself as an *error* … and the *error* can ultimately cause a *failure*".[1] A resulting *malfunction* that has a *hazardous* effect represents a loss of *functional safety*.

Item

Within this standard, *item* is a key term. *Item* is used to refer to a specific system (or combination of systems) to which the ISO 26262 Safety Life Cycle is applied, that implements a function (or part of a function) at the vehicle level. That is, the *item* is the highest identified object in the process and is thereby the starting point for product-specific safety development under this standard.

Element

Either a system, a *component* (consisting of hardware parts and/or software units), a single hardware part or a single software unit — effectively, anything in a system that can be distinctly identified and manipulated.

Fault

Abnormal condition that can cause an *element* or an *item* to fail.

Error

Discrepancy between a computed, observed or measured value or condition, and the true, specified or theoretically correct value or condition.

Failure

Termination of an intended behaviour of an *element* or an *item* due to a *fault* manifestation.

Fault Tolerance

Ability to deliver a specified functionality in the presence of one or more specified *faults*.

Malfunctioning Behaviour

Failure or unintended behaviour of an *item* with respect to its design intent.

Hazard

Potential source of *harm* (physical injury or health damage) caused by malfunctioning behaviour of the *item*.

Functional Safety

Absence of unreasonable risk due to *hazards* caused by malfunctioning behaviour of Electrical/Electronic systems.

Note: In contrast to other *Functional Safety* standards and the updated ISO 26262:2018, *Fault Tolerance* was not explicitly defined in ISO 26262:2011 - since it was assumed impossible to comprehend all possible faults in a system.[4]

Note: ISO 26262 does not use the IEC 61508 term Safe failure fraction (SFF). The terms *single point faults metric* and *latent faults metric* are used instead.[5]

Part 2: Management of functional safety [edit]

ISO 26262 provides a standard for functional safety management for automotive applications, defining standards for overall organizational safety management as well as standards for a safety life cycle for the development and production of individual automotive products.[6][7][8][9] The ISO 26262 safety life cycle described in the next section operates on the following safety management concepts:[1]

Hazardous Event

A *hazardous event* is a relevant combination of a vehicle-level *hazard* and an operational situation of the vehicle with potential to lead to an accident if not controlled by timely driver action.

Safety Goal

A *safety goal* is a top-level safety requirement that is assigned to a system, with the purpose of reducing the risk of one or more *hazardous events* to a tolerable level.

Automotive Safety Integrity Level

An *Automotive Safety Integrity Level* (ASIL) represents an automotive-specific risk-based classification of a *safety goal* as well as the validation and confirmation measures required by the standard to ensure accomplishment of that goal.

Safety Requirement

Safety requirements include all *safety goals* and all levels of requirements decomposed from the safety goals down to and including the lowest level of functional and technical safety requirements allocated to hardware and software components.

Parts 3-7: Safety Life Cycle [edit]

Processes within the ISO 26262 *safety life cycle* identify and assess hazards (safety risks), establish specific safety requirements to reduce those risks to acceptable levels, and manage and track those safety requirements to produce reasonable assurance that they are accomplished in the delivered product. These safety-relevant processes may be viewed as being integrated or running in parallel with a managed requirements life cycle of a conventional Quality Management System:[10][11]

1. An *item* (a particular automotive system product) is identified and its top level system functional requirements are defined.
2. A comprehensive set of *hazardous events* are identified for the *item*.
3. An *ASIL* is assigned to each *hazardous event*.
4. A *safety goal* is determined for each *hazardous event*, inheriting the ASIL of the hazard.
5. A vehicle level *functional safety concept* defines a *system architecture* to ensure the *safety goals*.
6. *Safety goals* are refined into lower-level *safety requirements*.
   (In general, each safety requirement inherits the ASIL of its parent safety requirement/goal. However, subject to constraints, the inherited ASIL may be lowered by decomposition of a requirement into redundant requirements implemented by sufficiently independent redundant components.)
7. "Safety requirements" are allocated to *architectural components* (subsystems, hardware components, software components)
   (In general, each component should be developed in compliance with standards and processes suggested/required for the highest ASIL of the safety requirements allocated to it.)
8. The architectural components are then *developed* and *validated* in accord with the allocated safety (and functional) requirements.

Part 8: Supporting Processes [edit]

ISO 26262 defines objectives for integral processes that are supportive to the Safety Life Cycle processes, but are continuously active throughout all phases, and also defines additional considerations that support accomplishment of general process objectives.

- Controlled corporate interfaces for flow down of objectives, requirements, and controls to all suppliers in distributed developments
- Explicit specification of safety requirements and their management throughout the Safety Life Cycle
- Configuration control of work products, with formal unique identification and reproducibility of the configurations that provides for traceability between dependent work products and identification of all changes in configuration
- Formal change management, including management of impact of changes on safety requirements, for the purposes of assurance of removal of detected defects as well as for product change without introduction of hazards
- Planning, control, and reporting of the verification of work products, including review, analysis, and testing, with regression analysis of detected defects to their source
- Planned identification and management of all documentation (work products) produced through all phases of the Safety Life Cycle to facilitate continuous management of functional safety and safety assessment
- Confidence in software tools (qualification of software tools for the intended and actual use)
- Qualification of previously developed software and hardware components for integration in the currently developed ASIL item
- Use of service history evidence to argue that an item has proven sufficiently safe in use for the intended ASIL

Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analysis [edit]

Main article: Automotive Safety Integrity Level
See also: Comparison of ASIL with Other Hazard Level Standards

Automotive Safety Integrity Level refers to an abstract classification of inherent safety risk in an automotive system or elements of such a system. ASIL classifications are used within ISO 26262 to express the level of risk reduction required to prevent a specific hazard, with ASIL D representing the highest hazard level and ASIL A the lowest. The ASIL assessed for a given hazard is then assigned to the safety goal set to address that hazard and is then inherited by the safety requirements derived from that goal.[12]

ASIL Assessment Overview [edit]

The determination of ASIL is the result of *hazard analysis and risk assessment*.[13] In the context of ISO 26262, a hazard is assessed based on the relative impact of hazardous effects related to a system, as adjusted for relative likelihoods of the hazard manifesting those effects. That is, each hazardous event is assessed in terms of severity of possible injuries within the context of the relative amount of time a vehicle is exposed to the possibility of the hazard happening as well as the relative likelihood that a typical driver can act to prevent the injury.[14]

ASIL Assessment Process [edit]

At the beginning of the safety life cycle, hazard analysis and risk assessment is performed, resulting in assessment of ASIL to all identified hazardous events and safety goals.

Each *hazardous event* is classified according to the *severity* (S) of *injuries* it can be expected to cause:

Severity Classifications (S):

S0 No Injuries
S1 Light to moderate injuries
S2 Severe to life-threatening (survival probable) injuries
S3 Life-threatening (survival uncertain) to fatal injuries

Risk Management recognizes that consideration of the severity of a possible injury is modified by how likely the injury is to happen; that is, for a given hazard, a hazardous event is considered a lower risk if it is less likely to happen. Within the *hazard analysis and risk assessment* process of this standard, the likelihood of an injurious hazard is further classified according to a combination of *exposure* (E) (the relative expected frequency of the operational conditions in which the injury can possibly happen) and *control* (C) (the relative likelihood that the driver can act to prevent the injury).

Exposure Classifications (E):

E0 Incredibly unlikely
E1 Very low probability (injury could happen only in rare operating conditions)
E2 Low probability
E3 Medium probability
E4 High probability (injury could happen under most operating conditions)

Controllability Classifications (C):

C0 Controllable in general
C1 Simply controllable
C2 Normally controllable (most drivers could act to prevent injury)
C3 Difficult to control or uncontrollable

In terms of these classifications, an *Automotive Safety Integrity Level D* hazardous event (abbreviated *ASIL D*) is defined as an event having reasonable possibility of causing a life-threatening (survival uncertain) or fatal injury, with the injury being physically possible in most operating conditions, and with little chance the driver can do something to prevent the injury. That is, *ASIL D* is the combination of S3, E4, and C3 classifications. For each single reduction in any one of these classifications from its maximum value (excluding reduction of C1 to C0), there is a single-level reduction in the ASIL from *D*.[15] [For example, a hypothetical uncontrollable (C3) fatal injury (S3) hazard could be classified as *ASIL A* if the hazard has a very low probability (E1).] The ASIL level below *A* is the lowest level, *QM*. *QM* refers to the standard's consideration that below *ASIL A*; there is no safety relevance and only standard Quality Management processes are required.[13]

These Severity, Exposure, and Control definitions are informative, not prescriptive, and effectively leave some room for subjective variation or discretion between various automakers and component suppliers.[14][16] In response, the Society for Automotive Safety Engineers (SAE) has issued *J2980 - Considerations for ISO26262 ASIL Hazard Classification* to provide more explicit guidance for assessing Exposure, Severity and Controllability for a given hazard.[17]

See also [edit]

- Automotive Safety Integrity Level, comparison with other safety level systems
- ARP4754 (Guidelines For Development Of Civil Aircraft and Systems)
- DO-178C (Aerospace)
- IEC 61508 (Industrial/General, ISO 26262 is an adaption[18] with minor differences[19])
- ISO 60730[20] (Household)

References [edit]

1. ^ *a b c d* *ISO 26262-1:2018(en) Road vehicles — Functional safety — Part 1: Vocabulary* . International Standardization Organization.
2. ^ "ISO 26262 Software Compliance: Achieving Functional Safety in the Automotive Industry" white paper by Parasoft
3. ^ *ISO 26262-1:2018(en) Road vehicles — Functional safety — Part 10: Guidelines on ISO 26262* . International Standardization Organization.
4. ^ Greb, Karl; Seely, Anthony (2009). *Design of Microcontrollers for Safety Critical Operation (ISO 26262 Key Differences from IEC 61508)* (PDF). ARMtechcon. Archived from the original (PDF) on 2015-09-06.
5. ^ Boercsoek, J.; Schwarz, M.; Ugljesa, E.; Holub, P.; Hayek, A. (2011). *High-Availability Controller Concept for Steering Systems: The Degradable Safety Controller* (PDF). Recent Researches in Circuits, Systems, Communications and Computers. WSEAS. pp. 222-228. Retrieved 2016-04-17.
6. ^ ISO 26262-2:2011, "Management of functional safety" (Abstract)
7. ^ Greb, Karl (2012). *Functional Safety and ISO 26262* (PDF). The Applied Power Electronics Conference and Exposition, Industry Sessions. APEC. p. 9.[*dead link*]
8. ^ Blanquart, Jean-Paul; Astruc, Jean-Marc; Baufreton, Philippe; Boulanger, Jean-Louis; Delseny, Hervé; Gassino, Jean; Ladier, Gérard; Ledinot, Emmanuel; Leeman, Michel; Machrouh, Joseph; Quéré, Philippe; Ricque, Bertrand (2012). *Criticality categories across safety standards in different domains* (PDF). ERTS2 Congress. Embedded Real Time Software and Systems. pp. 3-4. Archived from the original (PDF) on 2016-04-17.
9. ^ ISO 26262-10:2012(E), "Guideline on ISO 26262", pp. 2-3.
10. ^ Min Koo Lee; Sung-Hoon Hong; Dong-Chun Kim; Hyuck Moo Kwon (2012). "Incorporating ISO 26262 Development Process in DFSS" (PDF). *Proceedings of the Asia Pacific Industrial Engineering & Management Systems Conference*: 1128 (Figure 2). Archived from the original (PDF) on 2013-09-15. Retrieved 2013-08-01.
11. ^ Juergen Belz (2011-07-28). *The ISO 26262 Safety Lifecycle* . Archived from the original on 2014-02-23.
12. ^ *Glossary, V2.5.0* (PDF). AUTOSAR. p. 19. Archived from the original (PDF) on 2014-02-22. Retrieved 2014-02-16.
13. ^ *a b* *ISO 26262-3:2011(en) Road vehicles — Functional safety — Part 3: Concept phase* . International Standardization Organization.
14. ^ *a b* Hobbs, Chris; Lee, Patrick (2013-07-09). *Understanding ISO 26262 ASILs* . Embedded Technologies. Penton Electronics Group. {{cite book}}: |magazine= ignored (help)
15. ^ Martínez LH, Khursheed S, Reddy SM. LFSR generation for high test coverage and low hardware overhead. IET Computers & Digital Techniques. 2019 Aug 21.UoL repository
16. ^ Van Eikema Hommes, Dr. Qi (2012). *Assessment of the ISO 26262 Standard, "Road Vehicles - Functional Safety"* (PDF). SAE 2012 Government/Industry Meeting. John A. Volpe National Transportation System Center: SAE. p. 9.
17. ^ *J2980 - Considerations for ISO 26262 ASIL Hazard Classification* . SAE International. Archived from the original on 2018-10-26.
18. ^ "Relationship between ISO 26262 and IEC 61508" . *ez.analog.com*. Retrieved 2021-04-11.
19. ^ "Automotive vs Industrial Functional Safety" . *ez.analog.com*. Retrieved 2021-04-11.
20. ^ "IEC 60730-1:2013+AMD1:2015+AMD2:2020 CSV | IEC Webstore" . *webstore.iec.ch*. Retrieved 2021-04-11.